

§ 233.6

12 CFR Ch. II (1–1–16 Edition)

to file a suspicious activity report to the appropriate authorities.

(g) The requirement of this part to establish and implement written policies and procedures applies only to the U.S. offices of participants in designated payment systems.

§ 233.6 Non-exclusive examples of policies and procedures.

(a) *In general.* The examples of policies and procedures to identify and block or otherwise prevent or prohibit restricted transactions set out in this section are non-exclusive. In establishing and implementing written policies and procedures to identify and block or otherwise prevent or prohibit restricted transactions, a non-exempt participant in a designated payment system is permitted to design and implement policies and procedures tailored to its business that may be different than the examples provided in this section. In addition, non-exempt participants may use different policies and procedures with respect to different business lines or different parts of the organization.

(b) *Due diligence.* If a non-exempt participant in a designated payment system establishes and implements procedures for due diligence of its commercial customer relationships in order to comply, in whole or in part, with the requirements of this regulation, those due diligence procedures will be deemed to be reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions if the procedures include the steps set out in paragraphs (b)(1), (b)(2), and (b)(3) of this section and subject to paragraph (b)(4) of this section.

(1) At the establishment of the account or relationship, the participant conducts due diligence of a commercial customer and its activities commensurate with the participant's judgment of the risk of restricted transactions presented by the customer's business.

(2) Based on its due diligence, the participant makes a determination regarding the risk the commercial customer presents of engaging in an Internet gambling business and follows either paragraph (b)(2)(i) or (b)(2)(ii) of this section.

(i) The participant determines that the commercial customer presents a minimal risk of engaging in an Internet gambling business.

(ii) The participant cannot determine that the commercial customer presents a minimal risk of engaging in an Internet gambling business, in which case it obtains the documentation in either paragraph (b)(2)(ii)(A) or (b)(2)(ii)(B) of this section—

(A) Certification from the commercial customer that it does not engage in an Internet gambling business; or

(B) If the commercial customer does engage in an Internet gambling business, each of the following—

(1) Evidence of legal authority to engage in the Internet gambling business, such as—

(i) A copy of the commercial customer's license that expressly authorizes the customer to engage in the Internet gambling business issued by the appropriate State or Tribal authority or, if the commercial customer does not have such a license, a reasoned legal opinion that demonstrates that the commercial customer's Internet gambling business does not involve restricted transactions; and

(ii) A written commitment by the commercial customer to notify the participant of any changes in its legal authority to engage in its Internet gambling business.

(2) A third-party certification that the commercial customer's systems for engaging in the Internet gambling business are reasonably designed to ensure that the commercial customer's Internet gambling business will remain within the licensed or otherwise lawful limits, including with respect to age and location verification.

(3) The participant notifies all of its commercial customers, through provisions in the account or commercial customer relationship agreement or otherwise, that restricted transactions are prohibited from being processed through the account or relationship.

(4) With respect to the determination in paragraph (b)(2)(i) of this section, participants may deem the following commercial customers to present a minimal risk of engaging in an Internet gambling business—

Federal Reserve System

§ 233.6

(i) An entity that is directly supervised by a Federal functional regulator as set out in § 233.7(a); or

(ii) An agency, department, or division of the Federal government or a State government.

(c) *Automated clearing house system examples.* (1) The policies and procedures of the originating depository financial institution and any third party processor in an ACH debit transaction, and the receiving depository financial institution and any third party processor in an ACH credit transaction, are deemed to be reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions if they—

(i) Address methods to conduct due diligence in establishing a commercial customer account or relationship as set out in § 233.6(b);

(ii) Address methods to conduct due diligence as set out in § 233.6(b)(2)(ii)(B) in the event that the participant has actual knowledge that an existing commercial customer of the participant engages in an Internet gambling business; and

(iii) Include procedures to be followed with respect to a commercial customer if the originating depository financial institution or third-party processor has actual knowledge that its commercial customer has originated restricted transactions as ACH debit transactions or if the receiving depository financial institution or third-party processor has actual knowledge that its commercial customer has received restricted transactions as ACH credit transactions, such as procedures that address—

(A) The circumstances under which the commercial customer should not be allowed to originate ACH debit transactions or receive ACH credit transactions; and

(B) The circumstances under which the account should be closed.

(2) The policies and procedures of a receiving gateway operator and third-party processor that receives instructions to originate an ACH debit transaction directly from a foreign sender are deemed to be reasonably designed to prevent or prohibit restricted transactions if they include procedures to be followed with respect to a foreign sender if the receiving gateway operator or

third-party processor has actual knowledge, obtained through notification by a government entity, such as law enforcement or a regulatory agency, that such instructions included instructions for restricted transactions. Such procedures may address sending notification to the foreign sender, such as in the form of the notice contained in appendix A to this part.

(d) *Card system examples.* The policies and procedures of a card system operator, a merchant acquirer, third-party processor, or a card issuer, are deemed to be reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions, if the policies and procedures—

(1) Provide for either—

(i) Methods to conduct due diligence—

(A) In establishing a commercial customer account or relationship as set out in § 233.6(b); and

(B) As set out in § 233.6(b)(2)(ii)(B) in the event that the participant has actual knowledge that an existing commercial customer of the participant engages in an Internet gambling business; or

(ii) Implementation of a code system, such as transaction codes and merchant/business category codes, that are required to accompany the authorization request for a transaction, including—

(A) The operational functionality to enable the card system operator or the card issuer to reasonably identify and deny authorization for a transaction that the coding procedure indicates may be a restricted transaction; and

(B) Procedures for ongoing monitoring or testing by the card system operator to detect potential restricted transactions, including—

(1) Conducting testing to ascertain whether transaction authorization requests are coded correctly; and

(2) Monitoring and analyzing payment patterns to detect suspicious payment volumes from a merchant customer; and

(2) For the card system operator, merchant acquirer, or third-party processor, include procedures to be followed

§ 233.6

12 CFR Ch. II (1–16 Edition)

when the participant has actual knowledge that a merchant has received restricted transactions through the card system, such as—

(i) The circumstances under which the access to the card system for the merchant, merchant acquirer, or third-party processor should be denied; and

(ii) The circumstances under which the merchant account should be closed.

(e) *Check collection system examples.* (1) The policies and procedures of a depository bank are deemed to be reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions, if they—

(i) Address methods for the depository bank to conduct due diligence in establishing a commercial customer account or relationship as set out in § 233.6(b);

(ii) Address methods for the depository bank to conduct due diligence as set out in § 233.6(b)(2)(ii)(B) in the event that the depository bank has actual knowledge that an existing commercial customer engages in an Internet gambling business; and

(iii) Include procedures to be followed if the depository bank has actual knowledge that a commercial customer of the depository bank has deposited checks that are restricted transactions, such as procedures that address—

(A) The circumstances under which check collection services for the customer should be denied; and

(B) The circumstances under which the account should be closed.

(2) The policies and procedures of a depository bank that receives checks for collection from a foreign banking office are deemed to be reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions if they include procedures to be followed by the depository bank when it has actual knowledge, obtained through notification by a government entity, such as law enforcement or a regulatory agency, that a foreign banking office has sent checks to the depository bank that are restricted transactions. Such procedures may address sending notification to the foreign banking office, such as in the form of the notice contained in the appendix to this part.

(f) *Money transmitting business examples.* The policies and procedures of an operator of a money transmitting business are deemed to be reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions if they—

(1) Address methods for the operator to conduct due diligence in establishing a commercial customer relationship as set out in § 233.6(b);

(2) Address methods for the operator to conduct due diligence as set out in § 233.6(b)(2)(ii)(B) in the event that the operator has actual knowledge that an existing commercial customer engages in an Internet gambling business;

(3) Include procedures regarding ongoing monitoring or testing by the operator to detect potential restricted transactions, such as monitoring and analyzing payment patterns to detect suspicious payment volumes to any recipient; and

(4) Include procedures when the operator has actual knowledge that a commercial customer of the operator has received restricted transactions through the money transmitting business, that address—

(i) The circumstances under which money transmitting services should be denied to that commercial customer; and

(ii) The circumstances under which the commercial customer account should be closed.

(g) *Wire transfer system examples.* The policies and procedures of the beneficiary's bank in a wire transfer are deemed to be reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions if they—

(1) Address methods for the beneficiary's bank to conduct due diligence in establishing a commercial customer account as set out in § 233.6(b);

(2) Address methods for the beneficiary's bank to conduct due diligence as set out in § 233.6(b)(2)(ii)(B) in the event that the beneficiary's bank has actual knowledge that an existing commercial customer of the bank engages in an Internet gambling business;

(3) Include procedures to be followed if the beneficiary's bank obtains actual knowledge that a commercial customer of the bank has received restricted

Federal Reserve System

§ 234.1

transactions through the wire transfer system, such as procedures that address

(i) The circumstances under which the beneficiary bank should deny wire transfer services to the commercial customer; and

(ii) The circumstances under which the commercial customer account should be closed.

§ 233.7 Regulatory enforcement.

The requirements under this part are subject to the exclusive regulatory enforcement of—

(a) The Federal functional regulators, with respect to the designated payment systems and participants therein that are subject to the respective jurisdiction of such regulators under section 505(a) of the Gramm-Leach-Bliley Act (15 U.S.C. 6805(a)) and section 5g of the Commodity Exchange Act (7 U.S.C. 7b-2); and

(b) The Federal Trade Commission, with respect to designated payment systems and participants therein not otherwise subject to the jurisdiction of any Federal functional regulators (including the Commission) as described in paragraph (a) of this section.

APPENDIX A TO PART 233—MODEL NOTICE

[Date]

[Name of foreign sender or foreign banking office]

[Address]

Re: *U.S. Unlawful Internet Gambling Enforcement Act Notice*

Dear [Name of foreign counterparty]:

On [date], U.S. government officials informed us that your institution processed payments through our facilities for Internet gambling transactions restricted by U.S. law on [dates, recipients, and other relevant information if available].

We provide this notice to comply with U.S. Government regulations implementing the Unlawful Internet Gambling Enforcement Act of 2006 (Act), a U.S. federal law. Our policies and procedures established in accordance with those regulations provide that we will notify a foreign counterparty if we learn that the counterparty has processed payments through our facilities for Internet gambling transactions restricted by the Act. This notice ensures that you are aware that we have received information that your institution has processed payments for Internet gambling restricted by the Act.

The Act is codified in subchapter IV, chapter 53, title 31 of the U.S. Code (31 U.S.C. 5361 *et seq.*). Implementing regulations that duplicate one another can be found at part 233 of title 12 of the U.S. Code of Federal Regulations (12 CFR part 233) and part 132 of title 31 of the U.S. Code of Federal Regulations (31 CFR part 132).

PART 234—DESIGNATED FINANCIAL MARKET UTILITIES (REGULATION HH)

Sec.

234.1 Authority, purpose, and scope.

234.2 Definitions.

234.3 Standards for payment systems.

234.4 Changes to rules, procedures, or operations.

234.5 Access to Federal Reserve Bank accounts and services.

234.6 Interest on balances.

AUTHORITY: 12 U.S.C. 5461 *et seq.*

SOURCE: 77 FR 45919, Aug. 2, 2012, unless otherwise noted.

§ 234.1 Authority, purpose, and scope.

(a) *Authority.* This part is issued under the authority of sections 805, 806, and 810 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) (Pub. L. 111-203, 124 Stat. 1376; 12 U.S.C. 5464, 5465, and 5469).

(b) *Purpose and scope.* This part establishes risk-management standards governing the operations related to the payment, clearing, and settlement activities of designated financial market utilities. In addition, this part sets out requirements and procedures for a designated financial market utility that proposes to make a change to its rules, procedures, or operations that could materially affect the nature or level of risks presented by the designated financial market utility and for which the Board is the Supervisory Agency (as defined below). The risk management standards do not apply, however, to a designated financial market utility that is a derivatives clearing organization registered under section 5b of the Commodity Exchange Act (7 U.S.C. 7a-1) or a clearing agency registered with the Securities and Exchange Commission under section 17A of the Securities Exchange Act of 1934 (15 U.S.C. 78q-1), which are governed by the risk-management standards promulgated by